UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,756	05/14/2001	Robert C. Gardiner	283_299	8889

7590 10/19/2006

WALL MARJAMA & BILINSKI
Suite 400
101 South Salina Street
Syracuse, NY 13202

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,756	GARDINER, ROBERT C.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,28-38,42-48,60 and 61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,28-38,42-48,60 and 61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 24 January 2006 with acknowledgement of an original application filing date of 14 May 2001.

2. Claims 1-16, 28-38, 42-48, 60, and 61 are currently pending in this application. Claims 1, 28, 42, 60, and 61 are independent claims. Claims 1, 28, 42, 60, and 61 have been amended. Amendment to the claims is accepted.

Response to Arguments

3. Applicant's arguments with respect to 1-16, 28-38, 42-48, 60, and 61 have been considered but they are not persuasive. The grounds of rejection have been changed due to amendment of the independent claims, however the same art that was used in the previous Office Action is utilized below. The previous rejection was a 35 U.S.C. 102(e) for claims 1, 8, 9, 12, 28, 29, 30, 36, 42, and 61, the rejection below for these claims is now a 35 U.S.C. 103(a) due to amendment to the independent claims.

Brief summary of prior art of records:

Nordenstam: discloses a secure distribution method of a private key from a distributing unit to a receiving unit. Some examples of receiving units and distributing units are personal computers, mobile telephones, personal digital assistants, palmtops, smart cards, key generators, set top boxes, even devices in vehicles such as cars and motorcycles. The distributing and receiving units use a communication interface some examples are conventional communication busses, radio links, infrared links, wireless LAN links such as Bluetooth, links over public networks or combination thereof. See col. 6, lines 28-39.

Nysen: discloses an enhanced backscatter RF-ID tag reader system and multiprotocol RF tag reader system. In addition, the present invention allows the use of spread spectrum technology to receive data from backscatter tags. Further, certain interactive tags which download information from the interrogation signal may also be compatible with the technique. See col. 4, lines 62-66.

Carloganu: discloses a method and apparatus for operating a set of resources under the control of a secure processor. Specifically, the invention discloses a means to test the authenticity of a secure command. See col. 2, lines 50-67.

Tuttle: discloses an enclosed transceiver that includes an integrated circuit. The enclosed transceiver includes control logic and memory for decoding and storing input information. See col. 2, lines 42-57.

In response to applicant's argument on page 9, "As quoted from Nysen, the RFID tag of Nysen has an effective range of at least 15 feet and not 1 meter as claimed by the Applicant. Furthermore, the Nysen signal range is designed for an entirely different purpose than that of the Applicant's claimed invention ... Conversely, the Nysen signal range is designed for discrimination of an RFID interrogation signal among other unwanted signals". The Examiner disagrees with argument for multiple reasons. First Nysen indicates that the distance can be tailored. Therefore it is obvious that the distance could be tailored to any distance, such as 1 meter or less. Second the discrimination in Nysen provides the same results as applicants secure transmission. Third the applicant is arguing the references individually when it is the combination of Nysen and Nordenstam that provide for the secure distribution of keys.

In response to applicant's argument beginning on page 9, "The Applicant's claimed invention involves subject matter relating to the secure transmission of an encryption key to an electronic terminal. The Nysen ('671) reference describes subject matter relating to an RF-ID tag reader ... Consequently, the subject matter of Nysen ('671) does not appear applicable to the subject matter of the Applicant's claimed invention". The Examiner disagrees with argument again the applicant is arguing the references individual when they should be looked at in combination. Nysen discloses a RFID tag and tag reader system, note this system is an obvious variation of the receiving and distributing unit in Nordenstam, see col. 6, lines 28-39. In addition Nysen indicates that this technology can be utilized in to download information. Distribution of an encryption key is an obvious variation of how the technology can be used, see col. 4, lines 62-66.

In response to applicant's argument on page 10, "Referring to Nordenstam ('263), Nordentstam fails to teach or suggest transmission of "a signal having an effective range of less than or equal to one meter". In fact Nordenstam does not appear to employ any sort of limited signal transmitting range for any purpose ... employs a limited signal transmitted range, limited power level, limited direction and angular range and polarity to provide for added security of the transmission of the encryption key. The Applicant and Nordenstam take entirely different approaches to provide security for the transmission of an encryption key". The Examiner disagrees with argument again for multiple reasons. First again the applicant is arguing the references individual when it is the combination that was used to teach the specifics of a signal transmission with range, power, angle, and polarity. Second Nordenstam does teach that the standard communication interface can utilize standard smartcard, card reader, or Bluetooth

technology, all of which is known in the art with signal transmission limitations. Third Nysen teaches that the signal strength can be varied in order to limit or specify the importance of a signal being transmitted see col. 8, line 63 col. 9, line 2. Fourth Nysen teaches that the launch and receiving transducers can be connected to different dipole antennas see col. 18, lines 6-12. Hence the direction of the signal sent and received can be in different directions. Fourth Nysen teaches polarity, i.e. direction can be controlled see above.

In response to applicant's argument beginning on page 10, "The Examiner states that claims 10-11 and 37-38 ... Preferable, the secured command format includes a message authentication code signature value calculated using an encryption key and at least a portion of the content of the secured command ... Carloganu does not transmit a test encryption key as claimed by the Applicant". The Examiner disagrees with argument and notes that the 'authentication code signature' is an obvious variation of a 'test encryption key'.

In response to applicant's argument beginning on page 11, "three basic criteria must be met to establish a prima facie case of obviousness ...Consequently, there appears to be no suggest or motivation within the Nordenstam ('263) reference to combine it with the Nysen ('671) reference and the subject matter of the Nysen ('671) reference would not teach or suggest all the claim limitation recited within claim 60". The Examiner disagrees with argument for multiple reasons. First both references contain a motivation to combine the references. Nordenstam teaches that the distributing unit can take the form of smartcards, palm, mobile device such as in vehicles. Nysen teaches that the technology can be utilized to distribute information. Second Nysen discloses that the invention is to improve the discrimination of signal from unwanted signals. This discrimination is another means to establish security.

In response to applicant's argument on pages 12, 'Furthermore, a hypothetical combination of the subject matter of the Nordenstam ('263) reference and the subject matter of the Nysen ('671) reference would not teach or suggest all of the claim limitations recited within claim 60 ... at a predetermined power level of less than or equal to 1mW is not taught by either the Nysen reference not the Nordenstam reference'. The Examiner disagree with argument Nysen teaches a predetermined power level, see col. Note signal strength is an obvious variation of power level. The 1mW factor has is accomplished in Nysen

In response to applicant's argument begging on page 13, "transmission of an RF signal in a direction that resides within an angular range of plus or minus 15 degrees or less of a predetermined direction" and "transmission of an RF signal having a predetermined polarity ... With respect to an angular range, both Nordenstam and Nysen are silent. With respect to polarity, Nysen states that "When the reference signal is one polarity, the modulated backscatter signal passes directly through the mixer. When the reference signal is of the opposite polarity, the modulated backscattered signal is inverted" ... Nysen does not employ polarity for a purpose of security, nor for installing an encryption key". The Examiner disagrees with arguments for multiple reasons. First as previously stated the references should be looked at in combination. Nordenstam teaches distributing an encryption key, Nysen teaches apparatus and method of an RFID tag and tag reader. Furthermore Nysen teaches all the limitations noted pertaining to signal transmission and reception. See above.

In response to applicant's argument beginning on page 14 with respect to the Nordenstam and Nysen combination these have been previously argued and answered above.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-9, 12, 28-36, 42-48, 60, and 61** are rejected under 35 U.S.C. 103(a) as being unpatentable over Nordenstam et al. U.S. Patent No. 6,711,263 (hereinafter '263) in view of Nysen U.S. Patent No. 6,433,671 (hereinafter '671).

As to independent claim 1, "A portable keying device that is configured for installing at least one encryption key into at least one electronic terminal, said portable keying device comprising:" is taught in '263 col. 9, line 64 through col. 10, lines 14;

"a memory device for storing at least one encryption key" is shown in '263 col. 10, lines 14-18;

"and a communications unit coupled to said memory device said communications unit being operative to transmit said at least one encryption key in a predetermined format to at least one electronic terminal" is disclosed in '263 col. 10, lines 19-29;

"said at least one electronic terminal includes a secure memory location for storing at least one data communications encryption key" is taught in '263 col. 4, lines 24-29;

"and is configured to employ said encryption key for the purpose of encrypting input data" is shown in '263 col. 8, lines 30-33;

the following is not explicitly taught in '263:

"said predetermined format including a signal having an effective transmitting range of less than or equal to a meter" however '671 teaches "The graphs of FIGS. 36 and 37 illustrate the advantages of the DSSS system. The first portion of the curve on FIG. 37 for a distance between 5 and 25 feet shows the usual falloff of signal strength obtained with a system of the prior art without using the spread spectrum signal modulation according to the invention. The curve has been normalized to show a maximum signal strength of 1.0 at 5 feet from the antenna ... Accordingly, it is very easy to discriminate between a desired signal 15 feet from the reader, and an unwanted signal, such as from an adjacent toll lane, which in most cases will be at least 25 feet away ... It is possible to tailor the distances in actual set up very accurately by locating the antenna at the desired distance from the tag even though the transmitter, receiver/detector and decoder are located somewhere else" in col. 34, line 42 through col. 35, line 13. Note since it is possible to tailor the distance in the actual set up an obvious variation would be to tailor the distance so that is equal or less than a meter.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 a method of distributing keys to include a means for the portable keying device to utilize a RF-ID tag that is compatible with existing methods. One of ordinary skill in the art would have been motivated to perform such a modification because of the many schemes known for encoding and decoding identification signals (see '671 col. 1, lines 18 et seq.). "A number of different schemes are known for encoding, transmitting and decoding identification signals from RF-ID tags. However, these schemes are generally incompatible, therefore requiring proprietary readers to accept encoded transmissions from tags

of the same vendor. Even where the transmission scheme is not proprietary, there is no standardization in the various RF-ID applications".

As to dependent claim 2, "wherein the communications unit includes a low power-close proximity RF transceiver" however '671 teaches "It is also an object of the invention to provide a method for interrogating a backscatter generating tag, comprising the steps of (a) generating an interrogation signal having a frequency within a interrogation band; (b) emitting an interrogation signal as a radio wave signal; (interacting the emitted radio wave signal with a backscatter generating tag; (receiving a radio frequency backscatter signal from the tag" in col. 8, lines 53-67. The motivation to combine '263 and '671 is the same as stated above in claim 1.

As to dependent claim 3, "wherein the predetermined format includes transmitting an RF signal at a predetermined power level" however '671 teaches transmitting a RF signal at a specified sign al strength in col. 8, lines 53-67 {Note "power level" has the same meaning as "signal strength"}. The motivation to combine '263 and '671 is the same as stated above in claim 1.

As to dependent claim 4, "wherein the predetermined power level is less than or equal to 1mW" however '671 teaches "In one embodiment, the voltage controlled oscillator 10 is controlled to produce a sinusoidal RF" in col. 14, lines 1-10. The motivation to combine '263 and '671 is the same as stated above in claim 1.

As to dependent claim 5, "wherein the RF signal has an effective range of less than or equal to a meter" however '671 teaches "The graphs of FIGS. 36 and 37 illustrate the advantages of the DSSS system. The first portion of the curve on FIG. 37 for a distance between 5 and 25 feet shows the usual falloff of signal strength obtained with a system of the prior art

without using the spread spectrum signal modulation according to the invention. The curve has been normalized to show a maximum signal strength of 1.0 at 5 feet from the antenna ... Accordingly, it is very easy to discriminate between a desired signal 15 feet from the reader, and an unwanted signal, such as from an adjacent toll lane, which in most cases will be at least 25 feet away ... It is possible to tailor the distances in actual set up very accurately by locating the antenna at the desired distance from the tag even though the transmitter, receiver/detector and decoder are located somewhere else" in col. 34, line 42 through col. 35, line 13. The motivation to combine '263 and '671 is the same as stated above in claim 1. Note since it is possible to tailor the distance in the actual set up an obvious variation would be to tailor the distance so that is equal or less than a meter.

As to dependent claim 6, "wherein the predetermined format includes transmitting an RF signal in a predetermined direction" however '671 teaches "Another transponder system provides separate launch and receiving transducers ... These surface acoustic wave pass beneath the receiving transducer 170 and continue on toward or more reflectors 172 in the direction indicated by the arrow 174" in col. 17, lines 64-67. The motivation to combine '263 and '671 is the same as stated above in claim 1.

As to dependent claim 7, "wherein the predetermined format includes transmitting an RF signal having a predetermined polarity" however '671 teaches the direction of the signal sent and received can be controlled in col. 18, lines 6-11. The motivation to combine '263 and '671 is the same as stated above in claim 1.

As to dependent claim 8, "wherein the at least one encryption key is installed in the electronic terminal in accordance with a predetermined protocol" is disclosed in '263 col. 6, lines 47-52.

As to dependent claim 9, "wherein the predetermined protocol includes: performing a handshaking routine, whereby the keying device and the electronic terminal exchange handshaking messages" is taught in '263 col. 4, lines 13-18;

"transmitting the at least one encryption key from the keying device to the electronic terminal in response to a successful handshaking routine" is shown in '263 col. 4, lines 18-25;

"validating the step of transmitting by re-transmitting the at least one encryption key from the electronic terminal to the keying device, whereby the keying device compares the transmitted data communications encryption key to the re-transmitted data communications encryption key; and storing the at least one data communications encryption key in the secure encryption key memory location in response to a successful step of validating" is disclosed in '263 col. 10, lines 46-53.

As to dependent claim 12, "wherein the secure encryption key memory location is a memory location in non-volatile memory" is shown in '263 col. 5, lines 16-35.

As to independent claim 28, "A method for installing an encryption key in an electronic terminal, the electronic terminal including a secure encryption key memory location for storing the at least one encryption key, the method comprising:" is taught in '263 col. 9, line 64 through col. 10, lines 14;

"providing a portable keying device, whereby the portable keying device is physically separated from the electronic terminal" is taught in '263 col. 6, lines 33-38;

"performing a handshaking routine, whereby the keying device and the electronic terminal exchange handshaking messages" is taught in '263 col. 4, lines 13-18;

"transmitting an encryption key from the portable keying device to the electronic terminal" is shown in '263 col. 4, lines 18-25;

"and storing the encryption key transmitted from the portable keying device to the electronic terminal in the secure key memory location" is taught in '263 col. 4, lines 24-29.

As to dependent claim 29, "wherein the step of performing a handshaking routine includes transmitting an authorization signal from the portable keying device to the electronic terminal" is taught in '263 col. 4, lines 13-25

the following is not explicitly taught in '263:

"said predetermined format including a signal having an effective transmitting range of less than or equal to a meter" however '671 teaches "The graphs of FIGS. 36 and 37 illustrate the advantages of the DSSS system. The first portion of the curve on FIG. 37 for a distance between 5 and 25 feet shows the usual falloff of signal strength obtained with a system of the prior art without using the spread spectrum signal modulation according to the invention. The curve has been normalized to show a maximum signal strength of 1.0 at 5 feet from the antenna ... Accordingly, it is very easy to discriminate between a desired signal 15 feet from the reader, and an unwanted signal, such as from an adjacent toll lane, which in most cases will be at least 25 feet away ... It is possible to tailor the distances in actual set up very accurately by locating the antenna at the desired distance from the tag even though the transmitter,

receiver/detector and decoder are located somewhere else" in col. 34, line 42 through col. 35, line 13. Note since it is possible to tailor the distance in the actual set up an obvious variation would be to tailor the distance so that is equal or less than a meter.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 a method of distributing keys to include a means for the portable keying device to utilize a RF-ID tag that is compatible with existing methods. One of ordinary skill in the art would have been motivated to perform such a modification because of the many schemes known for encoding and decoding identification signals (see '671 col. 1, lines 18 et seq.). "A number of different schemes are known for encoding, transmitting and decoding identification signals from RF-ID tags. However, these schemes are generally incompatible, therefore requiring proprietary readers to accept encoded transmissions from tags of the same vendor. Even where the transmission scheme is not proprietary, there is no standardization in the various RF-ID applications".

As to dependent claim 30, "wherein the portable keying device provides the electronic terminal with a predetermined authorization code during the step of transmitting an authorization signal" is shown in '263 col. 8, lines 42-47.

As to dependent claim 31, "wherein the step of performing a handshaking routine includes transmitting RF signals having at least one predetermined transmission characteristic" disclosed in '671 col. 8, lines 53-67.

As to dependent claims 32-34, these claims contain substantially similar subject matter as claims 2-7; therefore they are rejected along similar rationale.

As to dependent claim 35, "wherein the at least one predetermined transmission characteristic includes transmitting an RF signal having a predetermined modulation format that is characterized by a predetennined programming voltage" is taught in '671 col. 14, lines 1-10 "In one embodiment, the voltage controlled oscillator 10 is controlled to produce a sinusoidal RF".

As to dependent claims 36, this claim is substantially similar to claim 9; therefore it is rejected along similar rationale.

As to independent claim 42, this claim is directed to a portable key installation system of the method of claim 28; therefore it is rejected along similar rationale.

As to dependent claims 43-48, these claims contain substantially similar subject matter as claims 2-7; therefore they are rejected along similar rationale.

As to independent claim 60, "A portable keying device for installing an encryption key into at least one electronic terminal, the portable keying device comprising:" is taught in '263 col. 9, line 64 through col. 10, lines 14;

"a memory device for storing the at least one encryption key" is shown in '263 col. 10, lines 14-18;

"and a communications unit coupled to said memory device, the communications unit being operative to transmit said at least one data communications encryption key to an electronic terminal according to a pre-determined format" is disclosed in '263 col. 10, lines 19-29;

"said electronic terminal including a secure memory location for storing said encryption key, said pre-determined format including at least one of: " is taught in '263 col. 4, lines 24-29;

the following is not specifically taught in '263:

"transmission of an RF signal at a predetermined power level of less than or equal to 1mW" however '671 teaches transmitting a RF signal at a specified signal strength in col. 8, lines 53-67 {Note "power level" has the same meaning as "signal strength"};

"transmission of an RF signal in a direction that resides within an angular range of plus or minus 15 degrees or less of a predetermined direction" however '671 teaches "Another transponder system provides separate launch and receiving transducers ... These surface acoustic wave pass beneath the receiving transducer 170 and continue on toward or more reflectors 172 in the direction indicated by the arrow 174" in col. 17, lines 64-67;

"the transmission of an lmW signal having a predetermined polarity" however '671 teaches the direction of the received and sent signal can be controlled in col. 18, lines 6-12.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 a method of distributing keys to include a means for the portable keying device to utilize a RF-ID tag that is compatible with existing methods. One of ordinary skill in the art would have been motivated to perform such a modification because of the many schemes known for encoding and decoding identification signals (see '671 col. 1, lines 18 et seq.). "A number of different schemes are known for encoding, transmitting and decoding identification signals from RF-ID tags. However, these schemes are generally incompatible, therefore requiring proprietary readers to accept encoded transmissions from tags of the same

vendor. Even where the transmission scheme is not proprietary, there is no standardization in the various RF-ID applications".

As to independent claim 61, "A portable keying device for installing an encryption key into at least one electronic terminal, the portable keying device including:" is taught in '263 col. 9, line 64 through col. 10, lines 14;

"a memory device for storing at least one encryption key" is shown in '263 col. 10, lines 14-18;

"and a communications unit coupled to said memory device said communications unit being operative to transmit said at least one encryption key via transmission of an RF signal" is disclosed in '263 col. 10, lines 19-41;

"and where said electronic terminal includes at least one of the following: a keypad, a signature pad, a card reader, a bar code reader, and a point of sail retail transaction processing apparatus" is taught in '263 col. 8, lines 42-47, col. 10, lines 2-6, and col. 10, lines 34-53;

the following is not explicitly taught in '263:

"said predetermined format including a signal having an effective transmitting range of less than or equal to a meter" however '671 teaches "The graphs of FIGS. 36 and 37 illustrate the advantages of the DSSS system. The first portion of the curve on FIG. 37 for a distance between 5 and 25 feet shows the usual falloff of signal strength obtained with a system of the prior art without using the spread spectrum signal modulation according to the invention. The curve has been normalized to show a maximum signal strength of 1.0 at 5 feet from the antenna ... Accordingly, it is very easy to discriminate between a desired signal 15 feet from the

reader, and an unwanted signal, such as from an adjacent toll lane, which in most cases will be at least 25 feet away ... It is possible to tailor the distances in actual set up very accurately by locating the antenna at the desired distance from the tag even though the transmitter, receiver/detector and decoder are located somewhere else" in col. 34, line 42 through col. 35, line 13. Note since it is possible to tailor the distance in the actual set up an obvious variation would be to tailor the distance so that is equal or less than a meter.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 a method of distributing keys to include a means for the portable keying device to utilize a RF-ID tag that is compatible with existing methods. One of ordinary skill in the art would have been motivated to perform such a modification because of the many schemes known for encoding and decoding identification signals (see '671 col. 1, lines 18 et seq.). "A number of different schemes are known for encoding, transmitting and decoding identification signals from RF-ID tags. However, these schemes are generally incompatible, therefore requiring proprietary readers to accept encoded transmissions from tags of the same vendor. Even where the transmission scheme is not proprietary, there is no standardization in the various RF-ID applications".

6. **Claims 10, 11, 37, and 38,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '263 in view of '671 in further view of Carloganu et al. U.S. Patent No. 6,226,749 (hereinafter '749).

As to dependent claim 10, the following is not disclosed in '263: **"wherein the step of validating includes transmitting a test encryption key from the keying device to the**

electronic terminal" however '749 teaches "Preferably, the secured command format includes a message authentication code signature value calculated using an encryption key and at least a portion of the content of the secured command. Command authentication testing is carried out by first calculating a test message authentication code signature value using one of the same or a paired encryption key stored in the security module and the same portion of the content of the secured command received by the security module. Following this, the message authentication code signature value in the secured command is checked to determine if it matches the test message authentication code signature value. If it matches, the command is authenticated; and if not, the command is declared to be faulty" in col. 3, lines 16-29.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 a method of distributing keys to include a means to test the encryption key used with the validation step. One of ordinary skill in the art would have been motivated to perform such a modification because due to the advances in communications with security modules a more flexible method is needed to insure communications are protected (see '749 col. 1, lines 57 et seq.). "This secured application program may be a single application program module or a plurality of application program modules, each of which may be invoked with a specific different security module command. It will be apparent that this prior art approach only allows the application software programmer to operate the secured resources using fixed program resources having predefined functionality. If the application software programmer wants to do other functions with the secured resources, a custom security module with additional secured application program modules would be required. In most cases the cost of such a customized security module would not be warranted by the added value that can be

achieved. The application software programmer must utilize duplicate resources (e.g. a second display or keypad) and control them directly by application processing unit 20. It is apparent that there is a need for a method and apparatus for operating a security module and associated resources in a more flexible and effective manner that allows an application software program running outside the security module to access critical resources controlled by the security module in a secured manner"

As to dependent claim 11, "wherein the electronic terminal compares the test data communications encryption key with a currently in-use data communications encryption key stored in the secure encryption key memory location" is taught in '749 col. 3, lines 16-29.

As to dependent claims 37 and 38, these claims are substantially similar to claims 10 and 11; therefore they are rejected along similar rationale.

7. **Claims 13-16,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '263 in view of '671 in further view of Tuttle et al. U.S. Patent No. 6,078,791 (hereinafter '791).

As to dependent claim 13, the following is not taught in the combination of '263 and '671: **"wherein the non-volatile memory includes E2PROM"** however '791 teaches "This memory includes, but is not limited to , PROMs, EPROMs, EEPROMs, SRAMs, DRAMs, and ferrorelectric memory devices" in col. 2, lines 46-49.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '263 and '671 a method of distributing secret keys with a distributing

device to include means to utilize various memory devices. One of ordinary skill in the art would have been motivated to perform such a modification because by utilizing various memory devices the packaging of the portable keying device can be varied to make inexpensive and readily manufactured in high volume products (see '791 col. 2 lines 8 et seq.) "In view of the problems described above and related problems that consequently become apparent to those skilled in the applicable arts, the need remains for enclosed electronic apparatus including transceivers wherein the enclosure is inexpensive, readily manufactured in high volume, appropriate in size for use as a stamp, label, or tag".

As to dependent claim 14, "wherein the non-volatile memory includes EPROM" is taught in '791 col. 2, lines 46-49.

As to dependent claim 15, "wherein the non-volatile memory includes Flash memory" is shown in '791 col. 7, lines 39-61.

As to dependent claim 16, "wherein the non-volatile memory includes battery-backed RAM" is disclosed in '791 col. 6, line 36 through col. 7, line 27.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Varadharajan et al.	U.S. Patent No. 5,887,063	issued dated: Mar. 23, 1999
Hashimoto	U.S. Patent No. 6,553,348	issued dated: Apr. 22, 2003

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to

expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 9:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen. Tran
Patent Examiner
Technology Center 2134
12 October 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100